IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF: BLACK SAMSUNG GALAXY A03 TRACPHONE (SM-S134DL), WITHOUT A CASE CURRENTLY LOCATED IN THE EVIDENCE STORAGE ROOM AT U.S. DEPARTMENT OF STATE, COMPUTER INVESTIGATIONS AND FORESNSICS DIVISION, 1400 WILSON BLVD, 12TH FLOOR, ARLINGTON, VA 22209	Case Nos. 2:23mj28-DAO_____

AFFIDAVIT IN SUPPORT OF APPLICATIONS UNDER RULE 41 FOR WARRANTS TO SEARCH AND SEIZE

I, Carrington Johnson, being duly sworn upon oath, hereby declare as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the examination of and the extraction of electronically stored information from one device —that is, a Samsung Galaxy A03 TracPhone, model SM-S134DL, black in color, without a case, that was recovered on December 16, 2022, from the personal possession of defendant CLEMENTE CASTRACUCCO ("CASTRACUCCO") at the time of his arrest—which is currently in the possession of law enforcement (hereinafter, the "Device").

2. I am a Special Agent with the Diplomatic Security Service ("DSS") of the United States Department of State. I have been employed as a Special Agent with DSS since May 2012. I have extensive training in identifying and investigating fraud schemes utilizing United States issued travel documents; passports and visas. Through both my training and experience, I have learned that fraudsters often use United States travel documents to effectuate their schemes. I am authorized to make arrests for violations of federal law.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other officers, agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

II. JURISDICTION

4. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

III. IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. I make this affidavit in support of applications for warrants to search the following device, which is currently in the possession of law enforcement in the evidence storage room at the U.S. Department of State, Computer Investigations and Forensics Division, 1400 Wilson Blvd, 12th Floor, Arlington, VA 22209:

a. a Samsung Galaxy A03 TracPhone, model SM-S134DL, black in color, without a case, recovered from defendant CASTRACUCCO at the time of his arrest on December 16, 2022, as more fully described in Attachment A;

(the "Device") for evidence, fruits, and instrumentalities of criminal offenses, including but not limited to, violations of 18 U.S.C. § 1344 (Bank Fraud) and 18 U.S.C. § 1028A (Aggravated Identity Theft). The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

6. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. § 1344

(Bank Fraud) and 18 U.S.C. § 1028A (Aggravated Identity Theft), have been committed by defendant CASTRACUCCO and others. There is also probable cause to search the Device, further described below and in Attachment A, for the things described in Attachment B.

IV. PROBABLE CAUSE

7. On March 1, 2023, a federal grand jury returned an indictment in case number 2:23-cr-00083-JNP charging defendant CASTRACUCCO with violations of 18 U.S.C. § 1344 (Bank Fraud) and 18 U.S.C. § 1028A (Aggravated Identity Theft).

8. The criminal violations charged in the indictment are predicated on the Defendant's scheme to defraud federally insured financial institutions by depositing forged checks into accounts at the victim banks, then proceeding to fraudulently withdraw funds from the bank accounts using account information and identification that did not belong to him. To effectuate his scheme, the Defendant presented United States Passport ID cards with his photograph but the personally identifying information of actual Utah residents who did not give the Defendant permission to use their identifications.

9. Defendant committee his scheme in Utah on November 8 and 9, 2022 and again on December 15 and 16, 2022, until he was arrested on December 16, 2022 in Saratoga Springs, Utah. Your affiant is aware that Defendant has committed the same scheme in numerous other states, including AL, CT, NY, OK, TX, WA, WI. Defendant was arrested on February 12, 2022 in the state of New York for a fraud scheme using fraudulent identifications, including United States Passport ID Cards.

10. Your affiant has reviewed numerous phone calls made by Defendant after he was booked into Utah County Jail on December 16, 2022. Your affiant learned that Defendant has co-conspirators and that he travels from New York to states all across the United States to

commit his scheme. Your affiant believes that Defendant uses his cell phone in furtherance of the scheme because on a phone call made between Defendant and an unidentified individual only known as "JAMIE" at 347-885-XXXX on January 30, 2023, the conversation revealed that she knew that the Defendant was arrested up in Utah, and that two others, J.P. and "Mutt" (yet to be identified) were all locked up in different states for doing similar schemes. In a phone call to F.S. at 718-881-XXXX on January 24, 2023, the Defendant told F.S. that "TJ" (yet to be identified) was waiting for him to post bail so they could return to New York. The defendant also talked about how TJ talks with an individual who goes by the name "SUPREME" who presumably controls their operations. The Defendant also explained to F.S. that soon the Defendant would work as a "driver", and earn 20% of the take from the banks, and not just the 10% that the Defendant was currently making. These phone calls among several others show there is a coordinated effort between multiple conspirators, many yet to be identified. Therefore, there is probable cause to believe that he used his phone in furtherance of the scheme and that evidence of the scheme will be located on his phone.

11. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know that the Devices are capable of and frequently used to communicate with other individuals, take and store photographs and videos, and used for internet searches, among other things. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device (and sometimes by implication who did not), as well as evidence relating to the commission of the offenses under investigation. For example, in my training and experience, individuals involved in interstate bank fraud and identity fraud frequently communicate with others using electronic devices about their criminal scheme.

12. The Device is currently in the lawful possession of law enforcement. The Device came into law enforcement's possession as part of a search incident to the arrest of CASTRACUCCO on December 16, 2022. I seek the additional warrant out of an abundance of caution to be certain that an examination of the Device complies with the Fourth Amendment and other applicable laws.

13. The Device is currently located in a law enforcement evidence storage room at the U.S. Department of State, Computer Investigations and Forensics Division, 1400 Wilson Blvd, 12th Floor, Arlington, VA 22209. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as it was when the Device first came into the possession of law enforcement.

V. TECHNICAL TERMS

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and

storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to

store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP

addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

15. Based on my training, experience, and research, I know that the Devices have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and/or PDA, and that it can access the Internet.

VI. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

17. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is

evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of execution.* Because the warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

VII. CONCLUSION

21. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Johnson, Carrington P

Digitally signed by Johnson, Carrington P
Date: 2023.03.29 15:46:46 -06'00'

Carrington Johnson, Affiant
Special Agent, Diplomatic Security Services

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Daphne A. Oberg

DAPHNE A. OBERG
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The items to be searched are:

a. a Samsung Galaxy A03 TracPhone, model SM-S134DL, black in color, without a case, that was recovered on December 16, 2022, from the personal possession of defendant CLEMENTE CASTRACUCCO ("CASTRACUCCO") at the time of his arrest.

(collectively, the "Device"). The Device is currently in the possession of law enforcement in the evidence storage room at the U.S. Department of State, Computer Investigations and Forensics Division, 1400 Wilson Blvd, 12th Floor, Arlington, VA 22209.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. § 1344 (Bank Fraud) and 18 U.S.C. § 1028A (Aggravated Identity Theft), for the time period February 16, 2022, through the present, including:

   a. Communications or other records concerning bank accounts and other financial records;
   b. Communications or other records concerning using the identities of other people;
   c. Communications or other records concerning the transfer of money to or among the Defendant and any third parties;
   d. Communication or other records concerning travel for the purpose of defrauding financial institutions and committing identity fraud;
   e. Communication or other records concerning United States Passport ID cards

2. Evidence indicating how and when the Device was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account user;

3. Evidence indicating the state of mind of the Device user as it relates to the crimes under investigation;

4. Evidence of the identity of the person(s) who used the Device;

5. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, text messages, instant messaging, electronic mail, documents, and browsing history;

6. Passwords, encryption keys, and other access devices that may be necessary to access the Device;

7. Records of or information about Internet Protocol addresses used by the Device; and

8. Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.